Journal of Korea Multimedia Society Vol. 14, No. 6, June 2011(pp. 775-784)

무인증서 공개키 암호에 기반한 다중수신자 암호 기법 및 응용

서 철[†], 박영호[††], 이경현[†††]

요 약

본 논문에서는 신원기반 다중수신자 암호 기법의 장점인 묵시적 인증을 제공하는 동시에 키 위탁문제를 해결하기 위한 무인증서 공개키 암호 기술 기반의 새로운 다중수신자 암호 기법을 소개한다. 제안 기법은 다중수신자에 대한 메시지 암호화 단계에서 겹선형 페어링 연산을 제거하였을 뿐만 아니라 복호화 단계에서 단 한 번의 겹선형 페어링 연산만을 요구하는 매우 효율적인 다중수신자 암호 기법이다. 또한, 본 논문에서는 제안 기법을 이용하여 스테이트리스 수신자 환경을 위한 서브셋-커버 프레임워크 기반의 새로운 공개키 브로드캐스트 암호 기법을 제시한다.

A Multi-receiver Certificateless Encryption Scheme and Its Application

Chul Sur[†], Youngho Park[††], Kyung Hyune Rhee[†††]

ABSTRACT

In this paper we introduce the notion of multi-receiver certificateless encryption that avoids the inherent key escrow problem of multi-receiver identity-based encryption, and also present a highly efficient multi-receiver certificateless encryption scheme which eliminates pairing computation to encrypt a message for multiple receivers. Moreover, the proposed scheme only needs one pairing computation to decrypt the ciphertext. Finally, we discuss how to properly transform our scheme into a new public key broadcast encryption scheme for stateless receivers based on the subset-cover framework, which enjoys the advantages of certificateless cryptography.

Key words: Multi-Receiver Encryption(다중수신자 암호), Certificateless Public Key Cryptography(무인증서 공개키 암호), Broadcast Encryption(브로드캐스트 암호), Bilinear Pairing(겹선형 페어링)

1. 서 론

일반적으로 송·수신자간 안전한 통신을 위하여 공개키 암호 기술을 사용할 경우 송신자는 수신자의 공개키로 메시지를 암호화하여 암호문을 수신자에게 전송한다. 수신자는 전송받은 암호문을 자신이 소유하고 있는 개인키로 복호화 하여 평문을 획득한다. 이와 같은 환경을 단일수신자 환경이라고 한다.

※ 교신저자(Corresponding Author) : 이경현, 주소 : 부산 남구 대연3동 599-1번지(608-737), 전화 : 051)629-6247, FAX : 051)626-4887, E-mail : khrhee@pknu.ac.kr
접수일 : 2010년 12월 28일, 수정일 : 2011년 5월 4일
완료일 : 2011년 6월 23일
[†] 준회원, 일본 큐슈대학교 박사후연구원
(E-mail : chulsur@itslab.csce.kyushu-u.ac.jp)
[††] 준회원, 부경대학교 박사후연구원
(E-mail : pyhoya@pknu.ac.kr)
[†††] 종신회원, 부경대학교 IT융합응용공학과
(E-mail : khrhee@pknu.ac.kr)
※ 이 논문은 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임. [NRF-2010-357-D00223]

이에 반하여, 다중수신자 환경에서의 공개키 암호 기법은 다음과 같다. n명의 수신자들은 각각 자신의 공개키 pk_i와 이에 대응하는 개인키 sk_i를 생성한다 (여기서 $i=1,...,n$이다). 송신자는 다중수신자 암호 기법 및 수신자의 공개키 집합 $(pk_1, ..., pk_n)$과 메시지 집합 $(M_1,..., M_n)$을 이용하여 암호문 집합 $(C_1,..., C_n)$을 생성한다. 각각의 수신자 i는 자신의 개인키 sk_i와 암호문 C_i을 입력 값으로 메시지 M_i를 복호화한다.

위와 같은 특성을 고려할 때, 다중수신자 암호 기법은 암호문을 공개된 채널상에서 특정 그룹의 수신자들에게 전송하는 디지털 컨텐츠의 안전한 분배 및 PayTV 시스템 등 여러 응용 분야에 활용되어질 수 있다. 이러한 응용 시스템에서, 다중수신자 암호 기법은 메시지 M을 보호하기 위하여 사용되어지는 세션키 K에 대한 암호화를 위하여 사용되어지며, 전체 암호문은 세션키 K를 암호화한 암호문과 메시지 M를 암호화한 암호문으로 구성되어진다.

또한, 다중수신자 암호 기법은 일반적인 브로드캐스트 암호 기법으로 변형되어질 수 있다[1]. 브로드캐스트 암호 기법은 메시지 송신자인 그룹 관리자 또는 브로드캐스터(Broadcaster)가 암호화된 데이터를 공개된 채널 상에서 특정 그룹의 수신자들에게 전송하며, 전송된 암호문은 단지 정당한 수신자들만이 복호화가 가능한 암호 기법이다. 특히, 메시지의 안전한 브로드캐스트를 위한 다중수신자 암호 기법은 신원기반 환경으로 쉽게 적용되어질 수 있다. 즉, 송신자는 메시지 M을 다중수신자의 신원정보들 ID_i을 이용하여 n번 암호화하여 암호문 $(C_1,...,C_n)$을 생성한 후 다중수신자에게 전송할 수 있다. 또한, 신원기반 다중수신자 암호 기법을 이용한 공개키 브로드캐스트 암호 기법은 공개키에 대한 묵시적 인증을 통하여 인증서 관리의 문제점을 해결할 수 있으므로, 최근 신원기반 다중수신자 암호 기법에 관한 연구가 크게 주목받고 있다[2,3].

하지만, 신원기반 암호시스템은 본질적으로 키 위탁문제를 내포하고 있기 때문에, 다중수신자 환경에서 신원기반 암호 기법은 저작권 요소의 분배와 같은 다양한 활용에 제한점을 지닌다. 그러므로, 다중수신자 환경에서 신원기반 암호 기법의 장점인 묵시적 인증을 유지하면서 키 위탁 문제를 해결할 수 있는 암호 기법에 대한 연구가 필요하다.

본 논문에서는 신원기반 다중수신자 암호 기법의 장점인 묵시적 인증을 제공하는 동시에 키 위탁문제를 해결하기 위한 무인증서 공개키 암호 기술 기반의 새로운 다중수신자 암호 기법을 소개한다. 제안 기법은 다중수신자에 대한 메시지 암호화 단계에서 겹선형 페어링(Bilinear Pairing) 연산을 제거하였을 뿐만 아니라 복호화 단계에서 단 한 번의 겹선형 페어링 연산만을 요구하므로 기 제안된 신원기반 다중수신자 암호 기법들 보다 높은 효율성을 제공한다. 또한, 본 논문에서는 제안 기법을 이용하여 스테이트리스(Stateless) 수신자 환경을 위하여 서브셋-커버(Subset-Cover) 프레임워크[4] 기반 새로운 공개키 브로드캐스트 암호 기법을 제시한다. 새롭게 제안된 브로드캐스트 암호 기법은 제안 다중수신자 암호 기법의 장점을 유지할 뿐만 아니라, 브로드캐스트 메시지에 대한 전송량은 기존의 기법[4]과 동일하다.

본 논문의 구성은 다음과 같다. 본 논문의 사전연구를 2장에서 소개하고, 3장에서는 무인증서 공개키 암호기반 다중수신자 암호 기법의 형식적 모델을 정의한 후, 겹선형 페어링을 이용한 제안 기법에 대하여 기술한다. 이후, 4장에서 제안 기법을 이용하여 스테이트리스 수신자 환경을 위한 새로운 공개키 브로드캐스트 암호 기법을 제시하고, 마지막으로 5장에서 결론을 맺는다.

2. 사전연구

2.1 다중수신자 암호 기술

다중수신자 환경에서는 송신자가 다중수신자에 해당하는 공개키들로 메시지를 암호화하여 다중수신자에게 브로드캐스트 형태로 전송한다. 각 수신자마다 다른 메시지를 암호화 할 수도 있고, 단일 메시지를 각 수신자에 해당하는 키로 암호화 할 수도 있다. 본질적으로, 다중수신자 암호 기술은 브로드캐스트 암호 기술로 변형되어질 수 있다.

다중수신자 암호 기술의 개념은 Baudron[5]와 Bellare[6]에 의해서 독립적으로 정의되었다. 그들의 주요 결론은 단일수신자 환경에서 안전한 공개키 암호 기법은 다중수신자 환경에서도 안전성을 보장한다는 것이다. 따라서, 안전한 다중수신자 암호 기법은 단일수신자 환경에서 안전한 암호 기법의 서로 다른 n개의 공개키로의 암호화로 구성되어질 수 있다.

예를 들어, ElGamal 암호 기법을 이용한 다중수신

자 암호 기법은 다음과 같다.

1. 각 수신자 i의 개인키 $x_i \in Z_q^*$와 공개키 g^{x_i}를 설정한다 (여기서 $i=1,...,n$으로 가정한다).
2. 임의의 $r_1,...,r_n \in Z_q^*$을 선택한다.
3. 각 수신자에 대한 암호문 $C_i=(g^{r_i}, g^{x_i \cdot r_i} \cdot M_i)$을 계산한다.

Kurosawa[7]는 위의 암호 기술보다 계산량과 데이터 전송량의 효율성을 향상시킨 "Randomness Re-use"라고 불리는 기술을 제안하였다. 즉, [7]에서 제안한 기술을 사용하면 단지 하나의 임의의 $r \in Z_q^*$만을 선택하고 다중수신자를 위한 암호문 $C_i=(g^r, g^{x_i \cdot r} \cdot M_i)$을 생성할 수 있다. 또한, [8]에서는 Kurosawa의 제안 기술을 재정의하고 "Randomness Re-use"를 이용하여 단일수신자 공개키 암호 기법이 다중수신자 공개키 암호 기법의 구성에 적합한 일반적인 방법을 제안하였다.

한편, Boneh와 Franklin의 실용적인 신원기반 암호 기법[9]의 제안으로 인하여 신원기반 다중수신자 암호 기법이 제안되었으며[10,11], 최근 겹선형 페어링을 기반으로 하는 효율적인 신원기반 다중수신자 암호 기법이 제안되었다[2]. 제안 기법은 기존의 신원기반 암호 기법을 다중수신자 암호 기법에 적용했을 때보다 겹선형 페어링 연산을 줄인 기법으로써 암호화 단계에서 한 번의 페어링 연산을 요구하고 복호화 단계에서 두 번의 페어링 연산을 요구한다.

2.2 무인증서 공개키 암호 기술

전통적인 공개키 기반구조(PKI, Public Key Infrastructure)에서는 사용자의 공개키와 신원정보간의 연관성을 명확하게 인증하기 위하여 신뢰기관(CA, Certificate Authority)에 의해 전자서명된 인증서를 사용한다. 하지만, 공개키 기반구조에서 사용자는 메시지를 수신자의 공개키로 암호화하기 전에 수신자의 인증서 상태 검증을 위한 절차를 수행해야 한다. 이러한 인증서 상태 검증을 위하여 인증서 폐지 목록(CRL, Certificate Revocation List) 또는 온라인 인증서 상태 검증 프로토콜(OCSP, Online Certificate Status Protocol)과 같은 기술들이 사용되어지고 있지만 이러한 대응 방안은 사용자 및 신뢰기관에게 많은 계산량 및 통신상의 오버헤드를 요구한다.

위에서 기술한 전통적인 공개키 기반구조의 문제점을 해결하기 위하여, 신원기반 암호 기술이 제안되었다. 신원기반 암호 기술은 사용자의 신원을 나타낼 수 있는 e-mail 주소, IP 주소, 주민등록번호 등을 공개키로 사용함으로써 공개키 기반구조에서의 공개키에 대한 인증을 생략하는 암호 기술이다. 따라서, 신원기반 암호 기술에서는 사전에 분배된 공개키 없이도 수신자의 알려진 신원정보를 활용하여 수신자에게 평문에 대한 암호문을 전송할 수 있다. 그러나, 신원기반 암호 기술에서는 수신자가 비밀키 생성 센터(PKG, Private Key Generation Center)로부터 비밀키를 전송받아야 하므로 본질적인 키 위탁문제를 내포하고 있어 비밀키 생성 센터는 사용자의 모든 암호문을 복호화 할 수 있다.

위와 같은 전통적인 공개키 기반구조 및 신원기반 암호 기술의 문제점을 해결하기 위하여, Al-Riyami와 Paterson은 전통적인 공개키 기반구조의 장점인 키 위탁문제를 해결하는 동시에 신원기반 암호 기술의 장점인 묵시적 인증을 제공할 수 있는 무인증서 공개키 암호 기술(Certificateless Public Key Cryptography)을 소개하였다[12]. 무인증서 공개키 암호 기술의 핵심 개념은 사용자의 개인키를 두 가지의 비밀 값을 결합하여 생성하는 것이다. 즉, 하나의 비밀 값은 사용자가 직접 생성하며 다른 비밀 값은 신원기반 암호 기술과 유사하게 키 생성 센터(KGC, Key Generation Center)가 생성하여 사용자에게 전송한다. 이러한 개인키 생성의 특성으로 무인증서 공개키 암호 기술은 키 위탁문제를 해결함과 동시에 묵시적 인증을 제공할 수 있다. 위와 같은 장점으로 인하여, 무인증서 공개키 암호 기술에 관한 연구가 최근까지 활발히 진행되고 있다[13-16].

2.3 겹선형 페어링 및 계산 복잡도 가정

본 절에서는 제안 기법을 설계하기 위한 기반기술로서 겹선형 페어링 및 관련 계산 복잡도 가정(Complexity assumption)을 소개한다. 제안 기법에 적용할 겹선형 페어링은 다음과 같이 설정된다[9,17].

1. G_1과 G_2는 위수(Order)가 소수 q인 곱셈 순환군(Multiplicative cyclic groups)이다.
2. g는 G_1의 생성자(Generator)이다.

3. $e: G_1 \times G_1 \rightarrow G_2$를 겹선형 함수(Map)라 한다.

위와 같은 겹선형 함수는 아래와 같은 두 가지 특성을 가진다.

1. Bilinear: 임의의 $u, v \in G_1$과 $a, b \in Z_q^*$에 대하여 식 $e(u^a, v^b) = e(u, v)^{ab}$을 만족한다.
2. Non-degenerate: $e(g, g) \neq 1_{G_2}$

또한, 식 $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$을 만족하기 때문에, $e(,)$은 대칭성(Symmetric)을 가진다.

제안 기법의 안전성은 다음과 같은 잘 알려진 계산 복잡도 가정에 기반하고 있다[17]. p-BDHI 문제(p-Bilinear Diffie-Hellman Inversion Problem)는 다음과 같이 정의된다. 입력 값으로 $(g, g^{\alpha}, ..., g^{\alpha^p}) \in G_1^{p+1}$이 주어졌을 때, 식 $e(g,g)^{1/\alpha} \in G_2$를 계산하는 문제이다. 알고리즘 B가 p-BDHI 문제를 해결하는데 이점 ϵ을 갖는다는 것은

$$\Pr\left[B(g, g^{\alpha}, ..., g^{\alpha^p}) = e(g,g)^{1/\alpha}\right] \geq \epsilon$$

로 정의한다. p-BDHI 가정은 아래와 같다.

• 정의 1. *(t, p, ϵ)-BDHI 가정이 G_1상에서 유효하다는 것은, t-시간을 갖고 G_1상에서 p-BDHI 문제를 해결하는 어떠한 알고리즘도 최대 ϵ 이상의 이점을 갖지 않는다는 것이다.*

3. 무인증서 공개키 암호기반 다중수신자 암호 기법

본 장에서는 무인증서 공개키 암호 기술을 기반으로 하는 다중수신자 암호(MR-CLE, Multi-receiver Certificateless Encryption) 기법의 형식적 모델을 제시한다. 이후, 겹선형 페어링을 이용하여 신원기반 다중수신자 암호 기법의 장점인 묵시적 인증을 제공함과 동시에 키 위탁문제를 해결한 무인증서 공개키 암호기반 다중수신자 암호 기법을 제안하고, 제안 기법에 대한 효율성에 관하여 논의한다.

3.1 형식적 모델

본 절에서는 단일수신자 환경에서 기 정의되었던 무인증서 공개키 암호 기술[12,13]을 다중수신자 환경으로 확장하기 위하여 새로운 무인증서 공개키 암호기반 다중수신자 암호 기법을 정의한다. 무인증서 공개키 암호기반 다중수신자 암호 기법의 정형화된 모델은 다음과 같다.

• 정의 2 (CL-PRE). *무인증서 공개키 암호기반 다중수신자 암호 기법은 아래와 같이 7가지의 알고리즘으로 구성된다.*

- Setup(k): 보안 매개변수 k를 입력 값으로, 마스터 키 mk와 공개 파라미터 $params$를 출력한다.
- Partial-Private-Key-Extract($params$, mk, ID): 공개 파라미터 $params$, 마스터 키 mk와 사용자의 신원정보 ID를 입력 값으로, 사용자에 대한 부분 개인키 d_{ID}를 출력한다.
- Set-Secret-Key($params$, ID): 공개 파라미터 $params$와 사용자의 신원정보 ID를 입력 값으로, 사용자에 대한 임의의 비밀 값 x_{ID}을 출력한다.
- Set-Private-Key($params$, d_{ID}, x_{ID}): 공개 파라미터 $params$, 사용자의 부분 개인키 d_{ID}와 비밀 값 x_{ID}을 입력 값으로, 사용자에 대한 개인키 sk_{ID}를 출력한다.
- Set-Public-Key($params$, x_{ID}): 공개 파라미터 $params$와 사용자의 비밀 값 x_{ID}을 입력 값으로, 사용자의 공개키 pk_{ID}를 출력한다.
- Encrypt(m, $params$, $(ID_1, ..., ID_n)$, $(pk_{ID_1}, ..., pk_{ID_n})$): 메시지 m, 공개 파라미터 $params$, 다중수신자에 대한 신원정보 $(ID_1, ..., ID_n)$와 공개키 $(pk_{ID_1}, ..., pk_{ID_n})$를 입력 값으로, 암호문 C을 출력하거나 에러 심볼 $\perp$을 출력한다.
- Decrypt($params$, sk_{ID}, C): 공개 파라미터 $params$, 암호문 C와 사용자의 개인키 sk_{ID}를 입력 값으로, 메시지 m을 출력하거나 에러 심볼 $\perp$을 출력한다.

제안 모델의 완전성(Completeness)으로서, $i \in [1,n]$에 대하여 아래와 같은 경우에만 암호문에 대한 정확한 메시지 m이 출력된다.

- Decrypt($params$, sk_{ID_i}, Encrypt(m, $params$, $(ID_1, ..., ID_n)$, $(pk_{ID_1}, ..., pk_{ID_n})$)) = m

여기서, $sk_{ID_i} \leftarrow$ Set-Private-Key($params$, d_{ID_i},

x_{ID_i})이다.

3.2 겹선형 페어링을 이용한 기법 설계

제안 MR-CLE 기법은 아래와 같은 7가지의 알고리즘으로 구성되어 있으며, 각 알고리즘의 자세한 설명은 다음과 같다.

• Setup: 보안 매개변수 k, k_0를 입력 값으로, 키 생성 센터(KGC)는 아래와 같은 절차를 수행한다.

1. k비트 소수 q를 선택하고, 위수 q를 갖는 군 (G_1, G_2)과 $e: G_1 \times G_1 \rightarrow G_2$를 생성한후 임의의 생성자 $g \in G_1$를 선택한다.
2. KGC의 마스터 키로 임의의 $\alpha \in Z_q^*$를 선택하고, 공개키 $g_1 = g^\alpha \in G_1$를 계산한다.
3. 암호학적 해쉬 함수들 $H_1 : \{0,1\}^* \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \rightarrow Z_q^*$, $H_3 : \{0,1\}^* \rightarrow \{0,1\}^{k_0+k_1}$를 선택하고, 그룹 원소 $g_2 = e(g,g) \in G_2$를 생성한다.

공개 파라미터는 $params = \{G_1, G_2, e, g_1, g_2, H_1, H_2, H_3\}$으로 구성하며 메시지 공간은 $M := \{0,1\}^{k_1}$이다.

• Partial-Private-Key-Extract: 공개 파라미터 $params$와 사용자 i의 신원정보 ID_i를 입력 값으로, $h_i = H_1(ID_i) \in Z_q^*$를 계산하고 사용자 i의 부분 개인키 $d_i = g^{1/(\alpha+h_i)} \in G_1$를 출력한다.

• Set-Secret-Value: 공개 파라미터 $params$와 사용자 i의 신원정보 ID_i를 입력 값으로, 임의의 $x_i \in Z_q^*$를 선택하고 사용자 i의 비밀 값으로 출력한다.

• Set-Private-Key: 공개 파라미터 $params$, 사용자 i의 부분 개인키 d_i와 비밀 값 x_i을 입력 값으로, 사용자 i의 개인키 $sk_i = (d_i, x_i) \in G_1 \times Z_q^*$를 출력한다.

• Set-Public-Key: 공개 파라미터 $params$와 사용자 i의 비밀 값 x_i을 입력 값으로, 사용자 i의 공개키 $pk_i = (pk_{i,1}, pk_{i,2}) = (g^{x_i}, g_1^{x_i}) \in G_1 \times G_1$를 출력한다.

• Encrypt: 송신자는 다중수신자의 신원정보 $(ID_1, ..., ID_n)$와 공개키 $(pk_1, ..., pk_n)$를 이용하여 메시지 $m \in M$의 암호문 C을 아래와 같은 단계를 통하여 출력한다.

1. $(pk_1, ..., pk_n)$가 G_1의 원소들인지 검사한 후, 만약 G_1의 원소가 아닌 경우에 $\perp$을 출력한다.
2. $h_1 = H_1(ID_i), ..., h_n = H_1(ID_n) \in Z_q^*$ 을 계산한다.
3. 임의의 $\sigma \in \{0,1\}^{k_0}$를 선택하고 $r = H_2(m \| \sigma \| L) \in Z_q^*$을 계산한 후, 아래와 같은 암호문 C를 생성한다.

$$C = (U_1, ..., U_n, V, L)$$
$$= ((pk_{1,1}^{h_1} \cdot pk_{1,2})^r, ..., (pk_{n,1}^{h_n} \cdot pk_{n,2})^r, (m \| \sigma) \oplus H_3(g_2^r), L)$$

여기서, L은 $\{U_1 \subset ID_1, ..., U_n \subset ID_n\}$와 같이 각 U_i에 관계되는 수신자 신원정보 ID_i를 나타내는 정보를 포함하고 있는 라벨(Label)이다.

• Decrypt: 암호문 C를 전송받은 수신자 $i \in [1,n]$는 아래와 같은 복호화 과정을 수행한다.

1. 암호문 C내의 L을 이용하여 수신자 i에 관계되는 U_i를 찾는다.
2. $h_i = H_1(ID_i) \in Z_q^*$를 계산한다.
3. $(m \| \sigma) = V \oplus H_3(e(d_i, U_i)^{1/x_i})$와 $r = H_2(m \| \sigma \| L)$을 계산한다.
4. 만약 식 $U_i = (pk_{i,1}^{h_i} \cdot pk_{i,2})^r$이 성립하면 m을 메시지로 출력하고, 그렇지 않으면 $\perp$을 출력한다.

제안 기법의 일치성 (Consistency)은 다음과 같이 증명할 수 있다.

$$\begin{aligned} e(d_i, U_i) &= e(g^{1/(\alpha+h_i)}, (g^{h_i \cdot x_i} \cdot g^{\alpha \cdot x_i})^r)^{1/x_i} \\ &= e(g^{1/(\alpha+h_i)}, g^{(h_i+\alpha) \cdot x_i \cdot r})^{1/x_i} \\ &= e(g,g)^r = g_2^r \end{aligned}$$

3.3 효율성

본 절에서는 제안 기법의 효율성에 관하여 논의한다. 제안 기법에서는 다중수신자의 수에 따라 메시지 m은 $((pk_{1,1}^{h_1} \cdot pk_{1,2})^r, ..., (pk_{n,1}^{h_n} \cdot pk_{n,2})^r, (m \| \sigma) \oplus H_3(g_2^r), L)$와 같이 암호화되므로, 제안 기법은 암호화 단계에서는 페어링 연산을 요구하지 않는다. 또한, 암호문에서 메시지 m을 획득하기 위한 복호화 단계에서는 $(m \| \sigma) = V \oplus H_3(e(d_i, U_i)^{1/x_i})$와 같이 한 번의 페어링 연산만을 요구한다. 따라서, 제안 기법은 암호화 단계에서 한번의 페어링 연산을 요구하며 복호화 단계에서 두 번의 페어링 연산을 요구하는 기 제안된 효율적인 신원기반 다중수신자 암호 기법[2]보다 높은 효율성을 가진다. 특히, 페어링을 이용한 암호 기법에서 페어링 연산을 줄이는 것은 매우 중요한 사항이

다. 왜냐하면, 페어링 연산은 아직까지 유한체상에서의 지수 연산과 같은 표준(Standard) 연산보다 많은 계산량을 요구하기 때문이다. 최근의 MIRACL 라이브러리 구현[18]에 따르면 512비트 Tate 페어링 연산은 20ms 시간이 소요되는 반면, 1024비트 모듈라(Modular) 상에서의 지수 연산은 8.80ms 시간이 소요된다.

4. 스테이트리스 수신자 환경을 위한 브로드캐스트 암호 기법으로의 응용

본 장에서는 공개키 브로드캐스트 암호 기술 및 스테이트리스 수신자 환경을 위해 제안된 서브셋-커버 프레임워크를 소개한 후, 3장에서 제안한 MR-CLE 기법을 이용하여 스테이트리스 수신자 환경을 위한 서브셋-커버 프레임워크 기반 새로운 공개키 브로드캐스트 암호 기법을 제시한다.

4.1 공개키 브로드캐스트 암호

브로드캐스트 암호 기술[1]은 메시지 송신자인 그룹 관리자 또는 브로드캐스터(Broadcaster)가 암호화된 데이터를 공개된 채널 상에서 특정 그룹의 수신자들에게 전송하며, 전송된 암호문은 단지 정당한 수신자들만이 복호화가 가능한 암호 기술이다. 최근 브로드캐스트 암호 기술은 디지털 컨텐츠의 분배 및 보호, 위성 기반의 비즈니스, 그룹 통신 등 여러 가지 응용 분야에 그 적용성이 폭 넓게 연구되고 있다. 이와 같은 어플리케이션에서의 주요 안전성 문제는 그룹에 가입한 정당한 구성원만이 그룹 통신에 접근할 수 있도록 하는 접근권한이다. 이러한 안전성 문제를 해결하기 위한 단순한 방법 중 하나는 그룹 구성원들에게 전송할 데이터를 정당한 그룹 구성원들만이 공통적으로 얻을 수 있는 그룹키로 암호화해서 전달하는 것이다. 즉, 그룹 데이터를 보호하기 위한 기술 중의 하나로 암호시스템을 사용하는 것이다.

브로드캐스트 암호 기술은 대칭키 브로드캐스트 암호 기법과 공개키 브로드캐스트 암호 기법으로 나누어질 수 있다. 대칭키 브로드캐스트 암호 기법에서는 그룹 관리자만이 데이터를 암호화하여 브로드캐스트 할 수 있지만, 공개키 브로드캐스트 암호 기법은 그룹 관리자 뿐만 아니라 그룹내 사용자들도 암호화된 데이터를 브로드캐스트 할 수 있는 특성으로 인하여 최근에는 공개키 브로드캐스트 암호 기법이 많은 주목을 받고 있다. 또한, 컴퓨터 및 기타 장치의 발달과 보편화로 인하여 일반 사용자들이 쉽게 콘텐츠를 만들 수 있게 되어, 공개키 브로드캐스트 암호 기법의 연구가 더욱 필요하다.

브로드캐스트 암호에서의 또 다른 중요한 이슈는 스테이트리스(Stateless) 수신자 환경을 위한 브로드캐스트 암호 기법에 관한 연구이다. 스테이트리스 수신자 환경이란 시스템 설정단계에서 시스템 사용자들에게 분배된 그룹키들이 시스템의 라이프타임동안 변경되지 않는 환경이다. 이러한 환경에서의 브로드캐스트 암호 기법을 위하여 논리적 트리 구조에 기반한 서브셋-커버(Subset-Cover) 프레임워크가 제안되었다[4]. 서브셋-커버 프레임워크에서는 먼저 부분 집합들 $S_1,...,S_w, S_j \subseteq N$ (여기서 N은 모든 사용자들의 집합을 나타낸다)을 정의한 후, 각 부분 집합 S_j에 대한 비밀키 L_j를 할당한다. 또한, 폐지된 사용자 집합 R이 발생하였을 경우, 정당한 사용자 집합은 $N \setminus R = \bigcup_{j=1}^{m} S_{i_j}$로 표현되며 브로드캐스터에 의해서 메시지를 암호화하기 위해 사용되는 세션키 K는 정당한 사용자 집합의 비밀키인 $L_{i_1},...,L_{i_m}$을 사용하여 암호화된다.

또한 [4]에서는, 서브셋-커버 프레임워크를 실현하기 위하여 Complete Subtree (CS) 기법과 Subset Difference (SD) 기법이 제안되었다. 제안 브로드캐스트 암호 기법은 CS 기법에 기반하여 설계되었으므로 본 논문에서는 CS 기법에 대하여 소개한다. CS 기법에서 각 사용자들은 완전이진트리 T의 리프(Leaf)로 나타내어지며, 서브셋-커버 패밀리 S는 T의 모든 완전서브트리들의 집합을 표현한다. 만약 v_j를 T의 노드라고 하면, v_j에 대한 T의 완전서브트리의 모든 리프들의 집합은 $S_j \in S$로 나타내어질 수 있다.

그림 1은 CS 기법의 키 설정 방식을 나타낸다. 예를 들어, 사용자 u_2는 자신의 노드와 상위 노드에 해당하는 비밀키 집합 $I_{v_9} = \{L_1, L_2, L_4, L_9\}$을 할당받는다.

만약 사용자 u_2가 수신 대상자에서 제외되면 브로드캐스터는 사용자 u_2가 가지고 있지 않은 비밀키를 이용하여 메시지를 암호화한다. 즉, 사용자 u_5, u_6, u_7, u_8를 위하여 비밀키 L_3로 세션키 K를 암호화하고, 사용자 u_3, u_4를 위하여 비밀키 L_5로 세션키 K를 암호화한다. 마지막으로 u_1을 위하여 비밀키 L_8로 세션키

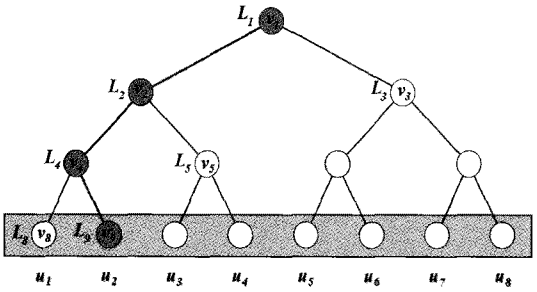

그림 1. CS 기법의 키 설정(|N|=8)

K를 암호화한다.

4.2 제안 MR-CLE를 이용한 스테이트리스 수신자 환경의 브로드캐스트 암호 기법

본 절에서는 3장에서 소개한 무인증서 공개키 암호기반 다중수신자 암호(MR-CLE) 기법을 이용하여 스테이트리스 수신자 환경을 위한 새로운 공개키 브로드캐스트 암호 기법을 제안한다. [4]에서 기술한 바와 같이 CS 기법은 스테이스리스 수신자 환경을 위한 공개키 브로드캐스트 암호에 적용되어질 수 있으며, 본 논문에서는 [3]에서 적용한 방법을 이용하여 제안 기법을 CS 기법에 기반한 새로운 공개키 브로드캐스트 암호 기법으로 확장한다.

먼저, 각 부분집합 S_i에 대한 신원정보 $ID(S_i)$를 다음과 같이 설정한다. 최상위노드로부터 하위노드로 내려오면서 왼쪽의 자식노드는 부모노드의 신원정보에 0을 추가하고, 오른쪽에 있는 자식노드는 1을 추가하도록 정의한다. 이후, 센터는 제안 MR-CLE 기법의 키 생성 센터의 역할을 수행하여 공개 파라미터 및 각 부분집합의 신원정보를 할당하기 위한 매핑 함수를 생성한 후, 모든 부분집합을 위한 부분 개인키를 생성한다. 이후, 각 사용자는 완전한 개인키 생성을 위하여 그림 2와 같이 비밀 값을 계산한다.

예를 들어, 각 사용자에 대응되는 단말노드가 v_j라면 비밀 값은 x_j이고 공개키는 $X_j = g_1^{x_j}$로 정의되어질 수 있다. 그림 2에서 사용자 u_2는 임의의 비밀 값 x_9를 선택한 후, 자신의 상위 노드 (v_4, v_2, v_1)의 개인키를 암호학적 해쉬함수 $H: G_1 \rightarrow Z_q^*$를 이용하여 다음과 같이 계산한다: $x_4 = H(X_8^{x_9})$, $x_2 = H(X_5^{x_4})$, $x_1 = H(X_3^{x_2})$. 위의 계산 값들의 결과로, 사용자 u_2만이 비밀 값 (x_1, x_2, x_4, x_9)을 계산할 수 있다.

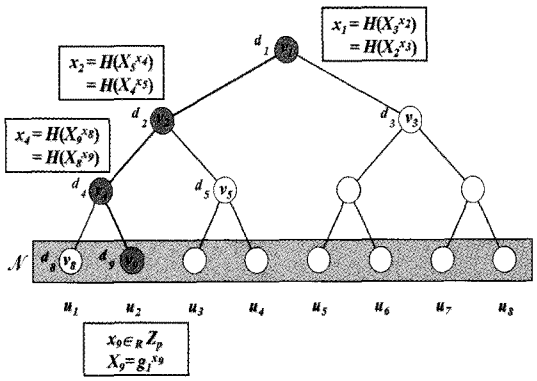

그림 2. 제안 기법의 키 설정(|N|=8)

지금부터 제안 MR-CLE 기법을 이용한 새로운 공개키 브로드캐스트 암호 기법에 대하여 설명한다. 제안 브로드캐스트 암호 기법은 아래와 같은 4가지의 알고리즘으로 구성된다[3].

- KeyGen: 센터는 마스터 키 mk와 공개 파라미터 $params$를 생성하기 위하여 MR-CLE 기법의 Setup 알고리즘을 실행한 후, 공개 파라미터 $params$와 각 부분집합에 신원정보를 할당하기 위한 매핑 함수 $ID(\cdot)$을 공개한다.
- Reg: 센터는 각 부분집합 $S_j \in S$에 부분 개인키 d_j를 할당하기 위하여 MR-CLE 기법의 Partial-Private-Key-Extract 알고리즘을 수행한다. 이후, 센터는 브로드캐스트된 암호문을 각 사용자가 복호화하기 위한 개인키 집합을 계산하기 위해 필요한 비밀정보 값 I_{v_j}를 해당 사용자에게 분배한다. 예를 들어, 그림 2에서 센터는 아래와 같이 사용자 u_2에게 비밀정보 값 I_{v_2}를 전송한다.

Center $\rightarrow u_2$: $I_{v_9} = \{d_1, d_2, d_4, d_9\}$

이후, 각 사용자는 임의의 비밀 값 x_j을 선택하고 개인키/공개키 쌍을 생성하기 위하여 MR-CLE 기법의 Set-Private-Key와 Set-Public-Key 알고리즘을 수행한다.

- Encrypt: 브로드캐스터는 메시지 m을 암호화하기 위해 사용된 세션키 K를 MR-CLE 기법의 Encrypt 알고리즘을 사용하여 암호화한 후, 그 결과로서 암호문을 출력하고 브로드캐스트 형태로 전송한다.
- Decrypt: 브로드캐스트된 암호문을 복호화 하

기 위하여, 정당한 수신자는 먼저 MR-CLE 기법의 Decrypt 알고리즘을 수행하여 세션키 K를 획득한 후, 세션키 K를 사용하여 메시지 m을 획득한다.

4.3 새로운 공개키 브로드캐스트 암호 기법 분석

기 제안되었던 스테이트리스 수신자 환경을 위한 공개키 브로드캐스트 암호 기법[2,3]에서는 센터가 공격자에 의해 손상되었을 경우, 신원기반 암호 기법의 키 위탁문제로 인하여 시스템내의 모든 개인키들이 손상된다. 그러므로, 시스템을 복구하기 위해서는 모든 부분집합에 해당하는 새로운 개인키를 생성해야 하지만, 스테이트리스 수신자 환경의 경우 수신자가 항상 온라인 상태를 유지하기 힘들므로 새로운 개인키 집합의 재분배에 많은 제약이 따른다. 이에 반하여, 본 논문에서 제안된 새로운 공개키 브로드캐스트 암호 기법은 신원기반 암호 기법에서의 키 위탁문제를 해결한 무인증서 공개키 암호 기술을 사용하였기 때문에, 위와 같은 상황이 발생하더라도 새로운 개인키 집합을 재분배할 필요가 없다. 또한 제안 기법은 신원기반 암호 기법의 장점인 묵시적 인증을 제공하므로 전통적인 PKI 기반 브로드캐스트 암호 기법이 내포하고 있는 인증서 관리문제를 해결할 수 있다.

효율성 측면에서, 제안 기법은 기 제안되었던 스테이트리스 수신자 환경을 위한 공개키 브로드캐스트 암호 기법[2,3]보다 계산량 측면에서도 보다 효율적이며, 제안 기법의 브로드캐스트 메시지에 대한 전송량은 기존의 기법[4]과 동일하다 (즉, $\mu \log N/\mu$, μ는 탈퇴자 수, N는 총 사용자 수).

5. 결 론

본 논문에서는 신원기반 다중수신자 암호 기법의 장점인 묵시적 인증을 제공하는 동시에 키 위탁문제를 해결하기 위한 무인증서 공개키 암호기반 다중수신자 암호 기법을 소개하였으며, 이를 위하여 새로운 기법 설계를 위한 형식적 모델을 정의한 후, 겹선형 페어링을 이용한 무인증서 공개키 암호기반 다중수신자 암호 기법을 제안하였다. 제안 기법은 다중수신자에 대한 메시지 암호화 단계에서 페어링 연산을 제거하였을 뿐만 아니라 복호화 단계에서 단 한번의 페어링 연산만을 요구하는 효율적인 기법이다. 뿐만 아니라, 제안 기법을 이용하여 모바일 환경과 같이 낮은 배터리 용량으로 장기간 온라인 상태를 유지할 수 없는 환경에 유용한 스테이트리스 수신자 환경을 위한 새로운 공개키 브로드캐스트 암호 기법을 제시하였다.

참 고 문 헌

[1] A. Fiat and M. Naor, "Broadcast Encryption," Advances in Cryptology - Crypto 1994, Springer, LNCS 773, pp. 480-491, 1994.

[2] J. Baek, R. Safavi-Naini, and W. Susilo, "Efficient Multi-Receiver Identity-Based Encryption and Its Application to Broadcast encryption," Public Key Cryptography - PKC 2005, Springer, LNCS 3386, pp. 380-397, 2005.

[3] Y. Dodis and N. Fazio, "Public Key Broadcast Encryption for Stateless Receivers," ACM-DRM 2002, 2002.

[4] D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Advances in Cryptology - Crypto 2001, Springer, LNCS 2139, pp. 41-62, 2001.

[5] O. Baudron, D. Pointcheval, and J. Stern, "Exteded Notions of Security for Multicast Public Key Cryptosystems," ICALP 2000, Springer, LNCS 1853, pp. 499-511, 2000.

[6] M. Bellare, A. Boldyreva, and S. Micali, "Public-Key Encryption in a Multi-User Setting: Security Proofs and Improvements," Advances in Cryptology - Eurocrypt 2000, Springer, LNCS 1807, pp. 259-274, 2000.

[7] K. Kurosawa, "Multi-Recipient Public-Key Encryption with Shortened Ciphertext," Public Key Cryptography - PKC 2002, Springer, LNCS 2274, pp. 48-63, 2002.

[8] M. Bellare, A. Boldyreva, and D. Pointcheval, "Multi-Recepient Encryption Schemes: Security Notions and Randomness Re-Use," Public Key Cryptography - PKC 2003, Springer, LNCS 2567, pp. 85-99, 2003.

[9] D. Boneh and M. Franklin, "Identity-Based

Encryption from the Weil Paring," Advances in Cryptology - Crypto 2001, Springer, LNCS 2139, pp. 213-229, 2001.

[10] L. Chen, K. Harrison, D. Soldera, and N. P. Smart, "Applications of Multiple Trust Authorities in Pairing Based Cryptosystems," InfraSec 2002, Springer, LNCS 2437, pp. 260-275, 2002.

[11] N. P. Smart, "Access Control Using Pairing Based Cryptography," CT-RSA 2003, Springer, LNCS 2612, pp. 111-121, 2003.

[12] S. S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," Advances in Cryptology - Asiacrypt 2003, Springer, LNCS 2894, pp. 452-473, 2003.

[13] S. S. Al-Riyami and K. Paterson, "CBE from CL-PKE: A Generic Construction and Efficient Scheme," Public Key Cryptography - PKC 2005, Springer, LNCS 3386, pp. 398-415, 2005.

[14] J. Baek, R. Safavi-Naini, and W. Susilo, "Certificateless Public Key Encryption Without Pairing," ISC 2005, Springer, LNCS 3650, pp. 134-148, 2005.

[15] B. Libert and J. Quisquater, "On Constructing Certificateless Cryptosystem from Identity Based Encryption," Public Key Cryptography - PKC 2006, Springer, LNCS 3958, pp. 474-490, 2006.

[16] 서철, 정채덕, 박영호, 이경현, "무인증서기반 프락시 재암호화 기법 및 다중 KGC 환경으로의 확장," 한국멀티미디어학회 논문지, 제12권, 4호, pp. 530-539, 2009.

[17] D. Boneh and X. Boyen, "Efficient Selective-Id Secure Identity Based Encryption Without Random Oracles," Advances in Cryptology - Eurocrypt 2004, Springer, LNCS 3027, pp. 223-238, 2004.

[18] MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library, http://indigo.ie/mscott.

서 철

2000년 부경대학교 전자계산학과 학사
2004년 부경대학교 전자계산학과 석사
2010년 부경대학교 전자계산학과 박사

2010년~현재 일본 류슈대학교 박사후연구원
관심분야 : 암호 프로토콜, 공개키 암호, 신원기반 암호

박 영 호

2000년 부경대학교 전자계산학과 학사
2002년 부경대학교 전자계산학과 석사
2006년 부경대학교 정보보호학과 박사

2010년~현재 부경대학교 박사후연구원
관심분야 : 암호 프로토콜, 암호기술 응용, 애드 혹 네트워크 보안

이 경 현

1982년 경북대학교 수학교육과 학사
1985년 한국과학기술원 응용수학과 석사
1992년 한국과학기술원 수학과 박사

1993년~현재 부경대학교 IT융합응용공학과 교수
관심분야 : 정보보호론, 공개키 암호, 신원기반 암호, 멀티미디어 정보보호, 그룹 키 관리